

Upper Bounds on the Size of Quantum Codes

Draft Version of 09.23.97

Alexei Ashikhmin

Los Alamos National Laboratory
Group CIC-3, Mail Stop P990
Los Alamos, NM 87545
e-mail: alexei@c3serve.c3.lanl.gov

Simon Litsyn

Department of Electrical Engineering-Systems
Tel Aviv University
Tel Aviv 69978, Israel
e-mail: litsyn@eng.tau.ac.il

Abstract

Several upper bounds on the size of quantum codes are derived using the linear programming approach. These bounds are strengthened for the linear quantum codes.

1 Introduction

Recently P.Shor presented a polynomial time algorithm for factoring large numbers on a quantum computer [19]. After this the interest in quantum computations grew dramatically. One of the crucial problems in implementation of quantum computer appeared to be the one of eliminating errors caused by decoherence and inaccuracy. Unlike the classical information, the quantum information can not be duplicated [20],[7]. Since error correcting codes protect classical information by duplicating it, their application for quantum information protection seemed to be impossible. However, in [18] P.Shor has shown that quantum error correction codes do exist and presented the first example of such one-error correcting code encoding one qubit to nine qubits. In [10] M.Knill and R. Laflamme formulated necessary and sufficient conditions for an error to be detectable by a given quantum

code, and thus introduced the notion of the minimum distance of a quantum code. In [17] P.Shor and R.Laflamme showed that, similarly to the classical codes, the quantum codes have enumerators related by the MacWilliams identities. Properties of quantum enumerators were extensively studied by E. Rains [14],[15],[16]. In particular, he showed that the minimum distance of the quantum code is determined by its enumerators. In [2],[3] a strong connection between a big class of quantum error-correction codes, which can be seen as an analog of classical linear codes, and self-orthogonal codes over $GF(4)$ was found.

A quantum code, say Q , of length n and dimension K , denoted as $((n, K))$ code, is a K -dimensional subspace of the Hilbert space \mathbf{C}^{2^n} . During transmission through a channel a code word can be altered by an error. In general a quantum channel error is an operator E acting on \mathbf{C}^{2^n} . If a codeword $\mathbf{v} \in Q$ has been effected by an error E then \mathbf{v} becomes $E\mathbf{v}$.

Here we consider one of the most popular channel models – the completely depolarized channel. In this model any error operator E can be represented in the form of the tensor product of Pauli matrices and two by two identity matrices

$$E = \sigma_1 \otimes \sigma_2 \otimes \dots \otimes \sigma_n, \quad (1)$$

and $\sigma_i \in \{\pm I_2, \pm\sigma_x, \pm\sigma_z, \pm\sigma_x\sigma_z\}$, where

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The error σ_x is called the flip error, and the error σ_z is called the phase error. Error operators acting on \mathbf{C}^{2^n} form the extraspecial group of order 2^{2n+1} . The number of nonidentity matrices in the tensor product (1) is called the weight of E and is denoted by $wt(E)$. A quantum code can detect an error E if and only if [10]

$$\mathbf{v}_i^\top E \mathbf{v}_j = 0,$$

where \mathbf{v}_i and \mathbf{v}_j are any two orthogonal vectors from the code. A quantum code has the minimum distance w and is denoted as $((n, K, w))$ code if it can detect any error of weight less than or equal to $w - 1$.

Linear codes play a special role in the classical coding theory. Similarly in the quantum coding theory there exist the, so called, stabilizer codes. They can be considered as an analog of the classical linear codes. The formal

definition of the quantum stabilizer codes is following. A quantum code Q is called stabilizer code if there exists a subgroup \mathcal{E} of the extraspecial group such that for $E\mathbf{v} = \mathbf{v}$ for any $\mathbf{v} \in Q$ and any $E \in \mathcal{E}$. In other words, Q forms an eigenspace of \mathcal{E} . If the group \mathcal{E} has the order 2^t then $\dim(Q) = 2^{n-t}$ and so the dimension of a stabilizer code is always equal to a power of 2. A nice property of the quantum stabilizer codes is that they are strongly related to classical self-orthogonal codes over $GF(4)$ [2][3]. Namely, there exists a quantum stabilizer $[[n, k]] = ((n, 2^k))$ code Q with the minimum distance w if and only if there exists a group self-orthogonal code C of length n , cardinality $|C| = 2^{n-k}$ such that $w = \min\{\text{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$, where C^\perp is the dual to C code with respect to the trace inner product. The trace inner product, denoted as $*$, of vectors \mathbf{v} and \mathbf{u} is defined as follows

$$\mathbf{v} * \mathbf{u} = \text{tr} \left(\sum_i v_i \overline{u_i} \right),$$

where the bar denotes conjugation in $GF(4)$. If code C , associated with quantum stabilizer code, is linear over $GF(4)$, then Q is called linear stabilizer code, or just linear quantum code.

A Gilbert-Varshamov type bound was obtained in [2].

Theorem 1 [4] *There exist quantum codes of length n and dimension K such that*

$$\frac{\log K}{n} \geq 1 - \frac{w}{n} \log 3 - H\left(\frac{w}{n}\right),$$

where $H(x) = -x \log x - (1-x) \log(1-x)$ is the binary entropy function and \log is the base 2 logarithm.

The goal of the present paper is to obtain upper asymptotic bounds on the minimum distance of an arbitrary quantum code using linear programming approach and some strengthenings of the bounds for linear quantum codes. For earlier known upper bounds see Laflamme and Knill [10], Rains [16], Cleve [5].

The paper is organized as follows. In section 2 we prove the key theorem that allows us to apply the linear programming approach to obtaining bounds for quantum codes. In section 3 we give a short description of properties of Krawtchouk polynomials that we will need later. In section 4.1 and 4.2 we use the key theorem to obtain Singleton and Hamming type bounds for arbitrary quantum codes. In section 4.3 we strengthen the Hamming type bound for the linear quantum codes.

2 The key inequality

In this section we obtain the key inequality allowing us to reduce the problem of upperbounding the size of codes to a problem of finding polynomials with special properties.

Like in the case of classical codes one can introduce the notion of enumerators of a quantum $((n, K))$ code. An $((n, K))$ quantum code Q has two enumerators [17],[14]

$$B_i = \frac{1}{K^2} \sum_{wt(E)=i}^n \text{Tr}(EP)\text{Tr}(EP),$$

$$B_i^\perp = \frac{1}{K} \sum_{wt(E)=i}^n \text{Tr}(EPEP),$$

where E is an error operator in \mathbf{C}^{2^n} . It is shown in [17],[14] that $0 \leq B_i \leq B_i^\perp$, $B_0 = B_0^\perp = 1$ and the values B_i and B_i^\perp are connected by MacWilliams identities, $B_i = \frac{1}{S} \sum_{t=0}^n B_t^\perp P_i(t)$, where $P_i(t)$ is the 4-ry Krawtchouk i -th polynomial and $S = \sum_{j=0}^n B_j^\perp$. In [17],[14] it is also shown that the minimum distance of Q equals the maximum integer w such that $B_i = B_i^\perp$, $i \leq w-1$. It is easy to check that $K = \frac{\sum_{j=0}^n B_j^\perp}{2^n} = \frac{S}{2^n}$, and thus we are interested in estimating the value w for given values n and S .

Let $f(x)$ be a polynomial of degree at most n ,

$$f(x) = \sum_{i=0}^n f_i P_i(x).$$

Let, moreover, all the coefficients f_i be nonnegative, $f(x) > 0$ for $x = 0, \dots, w-1$, and $f(x) \leq 0$ for $x = w, \dots, n$. Then

$$\begin{aligned} S \sum_{i=0}^{w-1} f_i B_i &\leq S \sum_{i=0}^n f_i B_i \\ &= S \sum_{i=0}^n \frac{1}{S} f_i \sum_{j=0}^n B_j^\perp P_i(j) = \sum_{j=0}^n B_j^\perp \sum_{i=0}^n f_i P_i(j) \\ &= \sum_{j=0}^n f(j) B_j^\perp \leq \sum_{j=0}^{w-1} f(j) B_j^\perp = \sum_{j=0}^{w-1} f(j) B_j. \end{aligned}$$

Thus,

$$\begin{aligned} S &\leq \frac{\sum_{j=0}^{w-1} f(j)B_j}{\sum_{j=0}^{w-1} f_j B_j} \\ &\leq \max_{j=0, \dots, w-1} \frac{f(j)}{f_j}. \end{aligned}$$

We formulate now the result as a theorem.

Theorem 2 *Let Q be an $((n, K, w))$ quantum code. Let*

$$f(x) = \sum_{i=0}^n f_i P_i(x)$$

be a polynomial, $f_i \geq 0$, and $f(x) > 0$ for $x = 0, \dots, w-1$, and $f(x) \leq 0$ for $x = w, \dots, n$. Then

$$K \leq \frac{S}{2^n} \leq \frac{1}{2^n} \max_{j=0, \dots, w-1} \frac{f(j)}{f_j}.$$

3 Krawtchouk polynomials

Here we survey some properties of Krawtchouk polynomials. We consider the quaternary case. In this case the Krawtchouk polynomials are defined as follows:

$$P_i(x) = \sum_{j=0}^i (-1)^j 3^{i-j} \binom{x}{j} \binom{n-x}{i-j}. \quad (2)$$

Every polynomial of degree at most n has a unique expansion in the basis of Krawtchouk polynomials. If a polynomial $f(x)$ has the expansion

$$f(x) = \sum_{i=0}^t f_i P_i(x),$$

then

$$f_i = 3^{-n} \sum_{j=0}^n f(j) P_j(i).$$

The following property (see [12] Chap. 5, Exercise 41) is important:

$$\sum_{i=0}^n \binom{n-i}{n-j} P_i(x) = 4^j \binom{n-x}{j}.$$

The Krawtchouk polynomials satisfy a recurrent relation,

$$(i+1)P_{i+1}(x) = (3n-2i-4x)P_i(x) - 3(n-i+1)P_{i-1}(x).$$

Some useful values of the Krawtchouk polynomials:

$$P_0(x) = 1, \quad P_1(x) = 3n - 4x, \quad 2P_2(x) = 16x^2 - 8x(3n-1) + 9n(n-1),$$

$$P_i(0) = 3^i \binom{n}{i}.$$

We will also need Christoffel-Darboux formula for binary Krawtchouk polynomials

$$\begin{aligned} & P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a) \\ &= \frac{2(a-x)}{t+1} \binom{n}{t} \sum_{i=0}^t \frac{P_i(x)P_i(a)}{\binom{n}{i}}. \end{aligned} \tag{3}$$

4 Upper bounds

In what follows we present several bounds derived from Theorem 2.

4.1 Singleton type bound

Choose in Theorem 2

$$f(x) = 4^{n-w+1} \prod_{j=w}^n \left(1 - \frac{x}{j}\right) = 4^{n-w+1} \frac{\binom{n-x}{n-w+1}}{\binom{n}{w-1}}.$$

Then

$$\begin{aligned} f_x &= 4^{-n} \sum_{j=0}^n f(j)P_j(x) \\ &= 4^{-w+1} \sum_{j=0}^n \frac{\binom{n-j}{n-w+1}}{\binom{n}{w-1}} P_j(x) \\ &= \frac{\binom{n-x}{w-1}}{\binom{n}{w-1}}. \end{aligned}$$

Now,

$$r(x) = \frac{f(x)}{f_x} = 4^{n-w+1} \frac{\binom{n-x}{n-w+1}}{\binom{n-x}{w-1}}.$$

Considering the ratio

$$\begin{aligned} \frac{r(x)}{r(x+1)} &= \frac{\binom{n-x}{n-w+1}}{\binom{n-x}{w-1}} \times \frac{\binom{n-x-1}{w-1}}{\binom{n-x-1}{n-w+1}} \\ &= \frac{n-x-w+1}{w-x-1}, \end{aligned}$$

we find that it is greater than 1 if $w \leq (n+2)/2$. So, the values $r(x)$ are decreasing, and we have the following theorem.

Theorem 3

$$K \leq \frac{1}{2^n} \frac{f(0)}{f_0} = 2^{n-2w+2}.$$

Note that though this bound has been already derived in [10],[16], the proof presented here is different and so could be of interest.

4.2 Hamming type bound

Let $e = (w-1)/2$. Define $f_x = (P_e(x))^2$.

Lemma 1

$$\begin{aligned} P_i(x)P_j(x) &= \\ \sum_{k=0}^n P_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-i-j} \binom{n-k}{s} \binom{2k+2s-i-j}{k+s-j} 2^{i+j-2s-k} 3^s. \end{aligned}$$

Proof The proof of the lemma is a straightforward generalization of the proof of the similar expression in the binary case (see e.g. [11](A.19)). \square

Using the lemma, we get

$$f_x = \sum_{k=0}^n P_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s.$$

This yields

$$f(x) =$$

$$\begin{aligned}
& \sum_{j=0}^n \sum_{k=0}^n \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s P_k(j) P_j(x) = \\
& \sum_{k=0}^n \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s \sum_{j=0}^{n-k} P_k(j) P_j(x) \\
& = 4^n \sum_{s=\max\{0, e-x\}}^{e-x/2} \binom{x}{2x+2s-2e} \binom{n-x}{s} \binom{2x+2s-2e}{x+s-e} 2^{2e-2s-x} 3^s.
\end{aligned}$$

Taking into account that

$$\frac{1}{n} \log \binom{n}{k} = H\left(\frac{k}{n}\right) + O\left(\frac{1}{n}\right),$$

and denoting $\xi = x/n$, $\nu = s/n$, and $\tau = e/n$, we get

$$\begin{aligned}
& \frac{1}{n} \log \left[\binom{x}{2x+2s-2e} \binom{n-x}{s} \binom{2x+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s \right] \\
& = \xi H\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) + (1-\xi) H\left(\frac{\nu}{1-\xi}\right) + \nu \log 3 + O\left(\frac{1}{n}\right).
\end{aligned}$$

Taking derivative of the last expression, we get

$$\begin{aligned}
& \frac{d \left(\xi H\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) + (1-\xi) H\left(\frac{\nu}{1-\xi}\right) + \nu \log 3 + O\left(\frac{1}{n}\right) \right)}{d\nu} \\
& = 2 \log \left(1 - \frac{2\xi+2\nu-2\tau}{\xi} \right) - 2 \log \left(\frac{2\xi+2\nu-2\tau}{\xi} \right) \\
& \quad + \log \left(1 - \frac{\nu}{1-\xi} \right) - \log \left(\frac{\nu}{1-\xi} \right) + \log 3.
\end{aligned}$$

It is not difficult to check that this function has only one root on the interval $\max\{0, \tau - \xi\} \leq \nu \leq \tau - \xi/2$. Let $\alpha(\tau, \xi)$ be the root of the function in the interval. Then we can estimate $\frac{1}{n} \log f(x)$ as follows

$$\begin{aligned}
& \frac{1}{n} \log f(x) \\
& = 2 + \xi + \xi H\left(\frac{2\xi+2\alpha(\tau, \xi)-2\tau}{\xi}\right)
\end{aligned} \tag{4}$$

$$+(1-\xi)H\left(\frac{\alpha(\tau, \xi)}{1-\xi}\right) + \alpha(\tau, \xi) \log 3 + O\left(\frac{1}{n}\right).$$

To obtain an estimate on f_x we need bounds on values of Krawtchouk polynomials. We will also need a bound on r_e , the smallest root of $P_e(j)$. For t growing linearly in n and $e = \tau n$ (see e.g. [8])

$$\xi_e = \frac{r_e}{n} = \frac{3}{4} - \frac{1}{2}\tau - \frac{1}{2}\sqrt{3\tau(1-\tau)} + o(1). \quad (5)$$

The next observation is a generalization of a similar fact in the binary case [9].

Lemma 2 *For $\xi < \xi_e$*

$$\frac{1}{n} \log P_e(x) = \frac{1}{n} \log \binom{n}{e} e^3 + \quad (6)$$

$$\int_0^\xi \log \left(\frac{3-2z-4\tau + \sqrt{(3-2z-4\tau)^2 - 12z(1-z)}}{6(1-z)} \right) dz + O\left(\frac{1}{n}\right).$$

Proof Like in the binary case (see, e.g. [12, Lemma 36]) one can show that for $\xi < \xi_t$

$$\frac{P_t(j+1)}{P_t(j)} = \frac{3n-2j-4t + \sqrt{(3-2j-4t)^2 - 12j(1-j)}}{6(1-j)} \left(1 + O\left(\frac{1}{n}\right)\right).$$

Taking logarithm on both sides, applying this recursively to $P_t(0) = \binom{n}{t} 3^t$, and approximating the sum by the integral, we get the claim. \square

Notice, that the integral in Lemma 2 can be expressed explicitly, namely

$$\begin{aligned} & \int \log \left(\frac{3-2z-4\tau + \sqrt{(3-2z-4\tau)^2 - 12z(1-z)}}{6-6z} \right) dz \\ &= -z \log 6 + (1-z) \log(1-z) + z \log(c+t) \\ &+ \frac{(a-1)}{4} \log(3+a-8z-2t) + \log(a-2) - \log 2 \\ &- \frac{1}{2} \log(6+2a-a^2-10z+2az-(a-2)t), \end{aligned}$$

where $a = 3 - 4\tau$, $c = a - 2z$, $t = \sqrt{c^2 - 12z(1-z)}$. Hence

$$\begin{aligned} \frac{1}{n} \log f_x &= 2\tau \log 3 + 2H(\tau) \\ &+ (-z \log 6 + (1-z) \log(1-z) + z \log(c+t)) \\ &+ \frac{(a-1)}{4} \log(3+a-8z-2t) + \log(a-2) - \log 2 \\ &- \frac{1}{2} \log(6+2a-a^2-10z+2az-(a-2)t) \Big|_0^\xi + O\left(\frac{1}{n}\right). \end{aligned} \quad (7)$$

Using Lemma 2, we can estimate $\frac{1}{n} \log f_x$ as follows

$$\begin{aligned} \frac{1}{n} \log f_x &= 2\tau \log 3 + 2H(\tau) \\ &+ \int_0^\xi \log \left(\frac{3-2z-4\tau + \sqrt{(3-2z-4\tau)^2 - 12z(1-z)}}{6-6z} \right) dz + O\left(\frac{1}{n}\right), \end{aligned}$$

Using (7) and (4), we get a Hamming type bound

$$\begin{aligned} &\frac{\log K}{n} \\ &\leq \max_{0 \leq \xi \leq \delta} \left\{ 1 + \xi + \xi H \left(\frac{2\xi + 2\alpha(\tau, \xi) - 2\tau}{\xi} \right) \right. \\ &\quad + (1-\xi) H \left(\frac{\alpha(\tau, \xi)}{1-\xi} \right) + \alpha(\tau, \xi) \log 3 - 2\tau \log 3 - 2H(\tau) \\ &\quad \left. - \int_0^\xi \log \left(\frac{3-2z-4\tau + \sqrt{(3-2z-4\tau)^2 - 12z(1-z)}}{6-6z} \right) dz \right\}, \end{aligned}$$

where $\delta = 2\tau = w/n$. Analytical computations with Maple show that this function achieves its maximum at $\xi = 0$ for any $\delta \leq \xi_e$. From this condition and (5) it follows that $\delta \leq \xi_e$ in the interval $0 \leq \delta \leq a$, $a \approx 0.34$.

Note that when $\delta \geq \xi_e$ the coefficient f_x can be equal to zero and the bound tends to infinity.

So we conclude that the conventional Hamming bound is valid when $\delta \leq 0.34$.

Theorem 4 *If Q is an $((n, K))$ quantum code and $\delta \leq \xi_e$, then*

$$\frac{\log K}{n} \leq 1 - \frac{\delta}{2} \log 3 - H\left(\frac{\delta}{2}\right).$$

Notice that would the Hamming type bound be proved for the total range, the value $\frac{\delta}{n}$ would be equal approximately to 0.38 when $\log(K)/n = 0$. This is worse than the bound $\delta/n \leq \frac{1}{3}$ derived by Rains in [16].

We labeled quantum Hamming bound on figure 1 by “H”. On the figure 1 we also present so called the first and the secon bounds (bounds LP1 and LP2), though for the time being it is not proved that they are valid. We shall prove in the next section that in the binary case the conventional first linear programming bound is valid for quantum codes.

4.3 The First Linear Programming Bound

In the present version of the paper we confine ourselves by the binary case. Work on the quaternary case is under process.

We formulate the problem the same as in the quaternary case. We have numbers B_i and B_i^\perp such that $0 \leq B_i \leq B_i^\perp$, B_i and B_i^\perp are connected by binary MacWilliams identities, and $(\sum_{i=0}^n B_i^\perp)(\sum_{i=0}^n B_i) = 2^n$. Let w be the first integer such that $B_{w-1} \leq B_{w-1}^\perp$. Denote $S = \sum_{i=0}^n B_i^\perp$. Like in the quaternary case we are interested in an upper bound for the value S given n and w .

Let

$$f(x) = \frac{1}{a-x} \{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\}^2.$$

This polynomial allows to get the so called first linear programming bound for classical codes [11]. Denote by $x_1^{(t)}$ the first root of the binary polynomial $P_t(x)$. To get the first linear programming bound one has to choose $\frac{t}{n} = \frac{1}{2} - \sqrt{\frac{\delta}{n}(1 - \frac{\delta}{n})} + o(1)$ and $x_1^{(t+1)} < a < x_1^{(t)}$, $\frac{P_t(a)}{P_{t+1}(a)} = -1$.

Using Christoffel-Darboux formula (3), one can write

$$\begin{aligned} f(x) &= \frac{2}{t+1} \binom{n}{t} \{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\} \\ &\quad \sum_{i=0}^t \frac{P_i(x)P_i(a)}{\binom{n}{i}} \\ &= \frac{2P_t(a)}{t+1} \binom{n}{t} \sum_{i=0}^t \frac{P_i(a)}{\binom{n}{i}} \{P_{t+1}(x)P_i(x) + P_t(x)P_i(x)\}. \end{aligned}$$

Using identity

$$P_r(x)P_s(x) = \sum_{j=0}^n P_j(x) \binom{n-j}{\frac{r+s-j}{2}} \binom{j}{\frac{r-s+j}{2}},$$

we get

$$\begin{aligned} f(x) &= \frac{2P_t(a)}{t+1} \binom{n}{t} \sum_{i=0}^t \frac{P_i(a)}{\binom{n}{i}} \left\{ \sum_{j=0}^n \binom{n-j}{\frac{t+1+i-j}{2}} \binom{j}{\frac{t+1-i+j}{2}} P_j(x) \right. \\ &\quad \left. + \sum_{j=0}^n \binom{n-j}{\frac{t+i-j}{2}} \binom{j}{\frac{t-i+j}{2}} P_j(x) \right\} \\ &= \sum_{j=0}^n P_j(x) \frac{2P_t(a)}{t+1} \binom{n}{t} \sum_{i=0}^t \frac{P_i(a)}{\binom{n}{i}} \left\{ \binom{n-j}{\frac{t+1+i-j}{2}} \binom{j}{\frac{t+1-i+j}{2}} \right. \\ &\quad \left. + \binom{n-j}{\frac{t+i-j}{2}} \binom{j}{\frac{t-i+j}{2}} \right\}. \end{aligned}$$

Suppose now that t and j are even numbers (in other cases arguments are similar). Estimate the sum in the last expression by the term for $i = t$. Then we have

$$f_j \geq \frac{2P_t^2(a)}{t+1} \binom{n-j}{\frac{2t-j}{2}} \binom{j}{\frac{j}{2}}.$$

Hence

$$\begin{aligned} \frac{f(x)}{f_x} &\leq \frac{\frac{1}{a-x} \{P_{t+1}(x)P_t(a) - P_t(x)P_{t+1}(a)\}^2}{\frac{2(P_t(a))^2}{t+1} \binom{n-x}{\frac{2t-x}{2}} \binom{x}{\frac{x}{2}}} \\ &= \frac{t+1}{2(a-x)} \frac{\{P_{t+1}(x) + P_t(x)\}^2}{\binom{n-x}{\frac{2t-x}{2}} \binom{x}{\frac{x}{2}}}. \end{aligned}$$

Replacing $P_t(x)$ by $P_x(t) \frac{\binom{n}{t}}{\binom{n}{x}}$ and $P_{t+1}(x)$ by $P_x(t+1) \frac{\binom{n}{t+1}}{\binom{n}{x}}$, we get

$$\begin{aligned} \frac{f(x)}{f_x} &\leq \frac{t+1}{2(a-x)} \frac{\{ \binom{n}{t+1} P_x(t+1) + \binom{n}{t} P_x(t) \}^2}{\binom{n-x}{\frac{2t-x}{2}} \binom{x}{\frac{x}{2}} \binom{n}{x}^2} \\ &= \frac{t+1}{2(a-x)} \frac{\binom{n}{t}^2 \{ \frac{n-t}{t+1} P_x(t+1) + P_x(t) \}^2}{\binom{n-x}{\frac{2t-x}{2}} \binom{x}{\frac{x}{2}} \binom{n}{x}^2}. \end{aligned}$$

Now using the relation [9]

$$\frac{P_x(t+1)}{P_x(t)} = \left(1 + O\left(\frac{1}{n}\right)\right) \frac{n-2x + \sqrt{(n-2x)^2 - 4x(n-x)}}{2n-2x}$$

and replacing $P_x(t)$ by $P_t(x)\frac{\binom{n}{x}}{\binom{n}{t}}$, we get

$$\begin{aligned} \frac{f(x)}{f_x} &\leq \frac{t+1}{2(a-x)} \frac{\binom{n}{t}^2 P_x(t)^2 \left\{ \frac{(n-t)(n-2x + \sqrt{(n-2x)^2 - 4x(n-x)})}{(t+1)(2n-2x)} + 1 \right\}^2}{\left(\frac{n-x}{2}\right) \left(\frac{x}{2}\right) \binom{n}{x}^2} \\ &= \frac{1}{2(a-x)} \frac{P_t(x)^2 \left\{ \frac{(n-t)(n-2x + \sqrt{(n-2x)^2 - 4x(n-x)}) + (t+1)(2n-2x)}{2(n-x)} \right\}^2}{(t+1) \left(\frac{n-x}{2}\right) \left(\frac{x}{2}\right)}. \end{aligned}$$

Using the estimate [9]

$$\frac{1}{n} \log P_t(x) = H(\tau) + \int_0^\xi \log \left(\frac{1-2\tau + \sqrt{(1-2\tau)^2 - 4z(1-z)}}{2-2z} \right) dz + o(1),$$

where $\xi = x/n$ and $\tau = t/n$, we have

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} \log \frac{f(x)}{f_x} &= 2H(\tau) + 2 \int_0^\xi \log \left(\frac{1-2\tau + \sqrt{(1-2\tau)^2 - 4z(1-z)}}{2-2z} \right) dz \\ &\quad - (1-\xi)H\left(\frac{2\tau-\xi}{2-2\xi}\right) - \xi. \end{aligned}$$

Analytical computations with Maple show that for $\tau \geq 0.11$ this function achieves its maximum at $\xi = 0$. Since $\delta = \frac{w}{n} = \frac{1}{2} - \sqrt{\tau(1-\tau)}$ we have the following theorem.

Theorem 5 *If $\delta \leq 0.1865$ then*

$$\frac{1}{n} \log S \leq H\left(\frac{1}{2} - \sqrt{\delta(1-\delta)}\right).$$

Note that we are interested in an estimate of w for all S such that $\frac{1}{n} \log S \geq 0.5$. Note also that when $\delta \leq 0.1865$ then $\frac{1}{n} \log S \approx 0.501$. So for all $1 \geq \frac{1}{n} \log S \geq 0.501$ the conventional first linear programming bound is valid.

4.4 Strengthening in Linear Case

Let now Q be a stabilizer quantum code with associated self-orthogonal code C over $GF(4)$. Recall that if $\dim(Q) = 2^k$ then $|C| = 2^{n-k}$.

A generator matrix of C can be written in the form [3]

$$G = \begin{bmatrix} I_{k_0} & \omega A_1 & B_1 \\ \omega I_{k_0} & \omega A_2 & B_2 \\ & I_{k_1} & A_3 \end{bmatrix}, \quad (8)$$

where B_j is a binary matrix, A_j is an arbitrary matrix, and ω is an element of $GF(4)$ of order 3. We will say that G defines a code of type $4^{k_0}2^{k_1}$. If in some l coordinates a group code, say D , of length n contains only 0-s and α -s, $\alpha \in GF(4), \alpha \neq 0$, then we will say that D is a mixed code of lengths l and $n-l$. Note that if C is a code of type $4^{k_0}2^{k_1}$ of length n then corresponding quantum stabilizer code Q is an $[[n, k]] = [[n, 2n - 2k_0 - k_1]]$ code.

Lemma 3 *The minimum distance w of Q is not greater than the minimum distance of the optimal group mixed code of lengths k_1 and $n - k_0 - k_1$ and cardinality $2^{2n-4k_0-2k_1}$. In particular*

i) *if $k_1 = 0$ then w is not greater than the minimum distance of the optimal group code of length $(n+k)/2$ and cardinality 4^k .*

ii) *if $k_1 < \frac{2n-4k_0}{3} = 2k$ then w is not greater than the minimum distance of the optimal group code of length $\frac{n+k-k_1}{2}$ and cardinality 2^{2k-k_1} .*

Proof

Let G_C be a generator matrix of the code C written in the form (8). Since $C \subseteq C^\perp$ we can append some rows to the matrix G_C to get a generator matrix of C^\perp . That is

$$G_{C^\perp} = \begin{bmatrix} G_C \\ G' \end{bmatrix}.$$

Let us call the code generated by the matrix G' a complementary code of C to C^\perp . It is clear that the minimum distance of a complementary code has to be not less than $w = \min\{\text{wt}(\mathbf{v}) : \mathbf{v} \in C^\perp \setminus C\}$. Due to the structure (8) of the matrix G we can make elements of G' on the first k_0 positions be equal to 0 and elements on the next k_1 positions be equal to 0 or ω . So G' will have the form $[0 \ D_1 \ D_2]$ where D_1 is an $2n - 4k_0 - 2k_1 \times k_1$ matrix consisting from 0-s and ω -s and D_2 is an arbitrary $2n - 4k_0 - 2k_1 \times n - k_0 - k_1$ matrix.

i) Follows from the previous.

ii) In the case $k_1 < \frac{2n-4k_0}{3}$ the matrix $[0 \ D_1 \ D_2]$ can be transformed to the form

$$\begin{bmatrix} 0 & A_1 & B_1 \\ 0 & 0 & B_2 \end{bmatrix},$$

where A_1 is an $k_1 \times k_1$ matrix consisting form 0-s and ω -s, B_1 and B_2 are arbitrary $k_1 \times n - k_0 - k_1$ and $2n - 4k_0 - 3k_1 \times n - k_0 - k_1$ matrices. Since the subcode with the generator matrix $[0 \ 0 \ B_2]$ has length $n - k_0 - k_1$, dimension $2n - 4k_0 - 3k_1$ and its minimum distance has to be not less than w the assertion follows. \square

Let D be a mixed code of lengths l and $n - l$ and dimension k . To get bounds for Q we have to get bound for the classical mixed code D . Plotkin and Hamming type bounds for mixed codes can formulated as follows.

Lemma 4

$$d \leq \frac{1}{2^k - 1} (l2^{k-1} + 3(n-l)2^{k-2}).$$

Proof

Let M be an array of all codewords of D . The total number of nonzero entries of M is equal to $l \cdot 2^{k-1} + (n-l) \cdot 3 \cdot 2^{k-2}$. Since the number of nonzero codewords in D is $2^k - 1$ we get the assertion. \square

Lemma 5

$$\sum_{i=0}^e \sum_{j=0}^i \binom{l}{j} 3^{j-i} \binom{n-l}{i-j} \leq 2^{2n-l-k},$$

where $e = \left\lceil \frac{d-1}{2} \right\rceil$.

Proof

Let F be the Cartesian product of $GF(2)^l$ and $GF(4)^{n-l}$. The volume V_e of a sphere of radius e in F is

$$V_e = \sum_{i=0}^e \sum_{j=0}^i \binom{l}{j} 3^{j-i} \binom{n-l}{i-j}$$

and the volume V of F is $2^l 4^{n-l}$. The number of codewords of D can not exceed the value V/V_e where $e = \left\lceil \frac{d-1}{2} \right\rceil$ and assertion follows. \square

Combining Lemma 4 and Lemma 3, we get a Plotkin type bound for a code of given type $4^{k_0} 2^{k_1}$.

Theorem 6

$$d \leq \frac{n+k}{2} \frac{3 \cdot 4^{k-1}}{4^k - 1} + \frac{k_1}{2} \frac{4^{k-1}}{4^k - 1}.$$

Combining Lemma 5 and Lemma 3, we get Hamming type bound for a code of given type $4^{k_0}2^{k_1}$.

Theorem 7

$$\sum_{i=0}^e \sum_{j=0}^i \binom{k_1}{j} 3^{j-i} \binom{n-k_0-k_1}{i-j} \leq 2^{2k_0+3k_1} = 4^{\frac{n-k}{2}+k_1},$$

where $e = \left\lceil \frac{d-1}{2} \right\rceil$.

Let now $k_1 = 0$. For example $k_1 = 0$ if the code C is linear. In this case a complementary code is not a mixed code. So applying the asymptotic version of the second linear programming bound [1] to this code we get a bound on the minimum distance of the code Q . One can see (bound S on fig.1) that this bound is better than the first linear programming and Hamming bounds on some interval.

Let $k_1 > 0$ and $n - k_1 < k < k_1/2$. Then according to Lemma 3 we can estimate the minimum distance of Q as the minimum distance of a group of length $\frac{n+k-k_1}{2}$ and cardinality 2^{2k-k_1} . For example, using the asymptotic bound from [1], we get bounds for $k_1 = 0, k_1 = 0.2, k_1 = 0.5$ on figure 2. So for small values of k_1 we still have some strengthening of the first linear programming and Hamming bounds on some interval.

References

- [1] M. J. Aaltonen, "A new bound on nonbinary block codes," *Discr. Math.*, vol. 83, pp. 139–160, 1990.
- [2] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, submitted.
- [3] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$," LANL e-print quant-ph/9608006.
- [4] A.R. Calderbank and P.W. Shor, "Good Quantum Error-Correcting Codes Exist, LANL e-print quant-ph/9512032.

- [5] R. Cleve, “Quantum stabilizer codes and classical linear codes,” LANL e-print quant-ph/9612048.
- [6] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, No. 10, 1973.
- [7] D. Dieks, “Communication by EPR devices,” *Phys. Lett. A*, **92**, 1982, p. 271.
- [8] V.I. Levenshtein, “Krawtchouk Polynomials and Universal Bounds for Codes and Designs in Hamming Spaces,” *IEEE Trans. on Inf. Theory*, **41**, no. 5, 1995, pp. 1303–1321.
- [9] G. Kalai and N. Linial, “On the distance distribution of codes,” *IEEE Trans. Inform. Theory*, vol. 42, pp.1467–1472, 1995.
- [10] E. Knill and R. Laflamme, “A theory of quantum error correcting codes,” LANL e-print quant-ph/9604034.
- [11] R. J. McEliece, E. R. Rodemich, H. Rumsey, Jr., and L. R. Welch, “New Upper Bounds on the Rate of a Code via the Delsarte-MacWilliams Inequalities,” *IEEE Trans. Inform. Theory*, vol. 23, pp.157–166, 1977.
- [12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1977.
- [13] F. J. MacWilliams and N. J. A. Sloane, and J. G. Thompson, “Good Self Dual Codes Exist,” *Discrete Math.*, **3**, 1972, pp.153–162.
- [14] E.M. Rains, “Quantum weight enumerators,” LANL e-print quant-ph/9612015.
- [15] E.M. Rains, “Nonbinary quantum codes,” LANL e-print quant-ph/97?.
- [16] E.M. Rains, “Quantum shadow enumerators,” LANL e-print quant-ph/961101.
- [17] P.W. Shor and R. Laflamme, “Quantum analog of the MacWilliams identities in classical coding theory,” LANL e-print quant-ph/9610040.
- [18] P.W. Shor, “Algorithms for quantum computation: Discrete logarithm and factoring,” *ibid*, p.124.

- [19] P.W. Shor, "Scheme for reducing decoherence in quantum memory,"
Phys. Rev. A, **52**, 1995, p. 2493
- [20] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned,"
Nature, **299**, 1982, p.802.

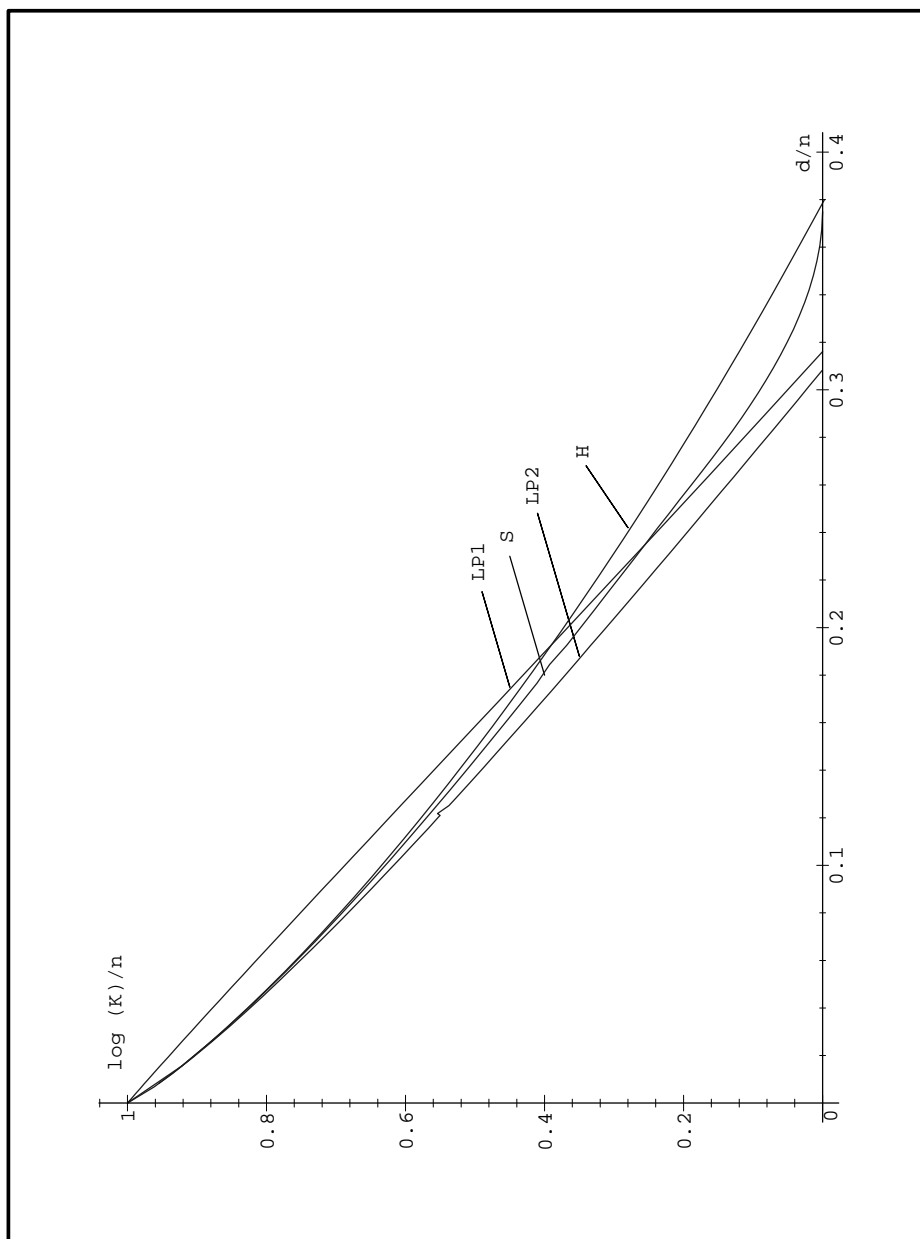


Figure 1: *LP1 and LP2 are the linear programming bounds ; H is Hamming type bound; S is strengthening for linear codes.*

